REMARKS

Claims 1-13 are pending in the instant application (hereinafter, the '320 Application), and stand rejected under one or more of 35 U.S.C. §112, first paragraph and 35 U.S.C. §102(e). The drawings are objected to as failing to comply with 37 C.F.R. §1.84(p)(5). The specification is objected to, due to lack of antecedent basis for an element of claim 5.

The drawings and the specification are amended to resolve the Examiner's objections. Claims 2 and 11 are amended to address and resolve the Examiner's §112 rejections. Claim 4 is amended to correct a typographical error. Claim 5 is amended for clarity, and claim 7 is amended to reflect the amendments to base claim 5. No new matter is added with these amendments, as noted herein below. It is believed that the above amendments and the following remarks are fully responsive to the 26 March 2007 Office Action.

Information Disclosure Statement

The Examiner notes that no information disclosure statement ("IDS") has been filed in the '320 Application. At this time, Applicants are unaware of any references that are material to patentability of the '320 Application. We note that the one patent cited in the specification of the '320 Application (U.S. 4,748,668) is listed in the Examiner's Notice of References cited. Since this patent is already of record, we submit that there is no need to list it in an IDS.

Drawings

The drawings were objected to as failing to comply with 37 C.F.R. §1.84(p)(5). In particular, the Examiner noted that reference numbers 12, 32 and 80 were not included in the written description. The objections to the drawings, along with other drawing issues noted by Applicants, are resolved as follows:

- FIG. 1 is amended to remove reference number 12. Note that reference number 12 indicated "Start" of method 10. The word "Start" remains in FIG. 1.
- FIG. 2 is amended to remove reference number 32, which indicated "Start" of method 30. The word "Start" remains in FIG. 2.
- The specification is amended to mention reference number 80, of FIG. 3.

- Likewise, the specification is amended to mention reference number 102, of FIG. 4.
- FIG. 4 is amended to label feature 94 as a "Connection Module," instead of a "Connection." Support for this clarifying amendment is found, for example, at paragraph [0026], found on pages 5-6 of the specification.
- In addition, all drawings are amended to correct page margins and text size, pursuant to 37 C.F.R. §§1.84(g) and (p)(3).

It is believed that the above-described amendments resolve the Examiner's objections to the drawings. We respectfully request acceptance of the five attached sheets of formal Replacement Drawings, and withdrawal of the Examiner's objection.

Specification

The Examiner objected to the specification as failing to provide proper antecedent basis for the claim 5 feature of "creating a prover agent application on the client". Respectfully, we submit that this feature is supported by the specification as filed. For example, the '320 Application recites that "authentication software (including authentication and prover agents) may be preloaded into each computer" desiring access to a network. p. 8, ¶[0033]. In addition, the '320 Application incorporates by reference U.S. Provisional No. 60/418,889 (the "parent provisional"), which further supports the objectionable feature of claim 5.

For example, claim 2 of the parent provisional also recites "creating a prover application on the client." Indeed, claim 2 of the parent provisional is identical to claim 5 of the '320 Application.

We believe that support for the objectionable claim 5 feature is already provided in the '320 Application, as filed and via incorporation-by-reference of the parent provisional. However, for clarity, the specification is amended herewith to add a paragraph describing the method presented in claim 5. Per MPEP §2163.06, "...information contained in any one of the specification, claims or drawings of the application as filed may be added to any other part of the application without introducing new matter." The amendment to the specification constitutes the addition of information from the claims into the specification, and is therefore acceptable and in

compliance with 35 U.S.C. §112, first paragraph. We respectfully request entry of this amendment, and withdrawal of the Examiner's objection to the specification.

We submit that the specification, including the paragraph added herewith, provides antecedent basis for claim 5.

Claim Objections

The Examiner objects to claim 11, stating that it recites "further comprising periodically and distributing." However, claim 11 does not include this language. We believe that the Examiner meant to reference claim 2; hence, claim 2 is amended herewith to recite "further comprising periodically generating and distributing..." Support for the amendment to claim 2 includes, but is not limited to, the following:

"Trusted source 106, FIG. 4, implements process 10, FIG. 1, to generate a new secret s" and a new product n" periodically to prevent the malicious party compromising the values by guessing or factoring. Thus, once computer system 536 has been authenticated and is connected to LAN 502 it receives new values for secret s" and product n", using an encrypted message based on its current values for secret s" and product n". Thus, integrity and security of system 500 is maintained at a high level. Only during initialization of system 500, or when a mobile computer (e.g., mobile computers 514, 516) connects to wireless LAN interface 512 and requests authentication, is a predefined secret used." pp. 8-9, ¶[0030]; FIG. 4.

The Examiner next objected to the recitation of "LAN" in claim 11. Accordingly, claim 11 is amended to recite a "local area network," per the Examiner's stipulation. Support for this amendment is found throughout the '320 Application. See, e.g., p. 1, ¶[0002], which assigns the abbreviation "LAN" to the term local area network.

Claim Rejections – 35 U.S.C. §112

Claim 5 stands rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. In particular, the Examiner states that the metes and bounds of "creating a prover/verifier agent application on the client/host" are unclear.

Prover and verifier agents on clients and hosts are well described in the '320 Application (See, e.g., Specification p. 5, ¶¶[0022]-[0023], among many other locations). We therefore

believe that the Examiner finds fault with the recitation of "creating" and not with the prover application, verifier application, client or host in particular.

Accordingly, claim 5 is amended to recite "installing" a prover/verifier agent application on the client/host. Support for the amendment to claim 5 is for example found at claim 8, which recites authentication agents and prover agents being installed on each of the computers through common software. In addition, "authentication, authentication software (including authentication and prover agents) may be preloaded into each computer (e.g., computers 514, 516, 518, 530, 534, 536)." Specification pp. 8-9, ¶[0033]. Further support for the amendment to claim 5 is found in the parent provisional, which recites "In initialization step 14 the initial value of secret (s-not prime "s") is generated from a seed value ***determined when agent is installed***". Parent provisional p. 2, ¶[0011], emphasis added.

It is believed that the amendment to claim 5 fully addresses and resolves the §112 rejection. We respectfully request entry of the amendment, and withdrawal of said rejection.

Claim Rejections – 35 U.S.C. §102

Claims 1-13 stand rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Application Publication No./ 2004/0008845 ("Le"). We respectfully disagree and traverse the rejection, since Le does not teach all limitations of the present claims.

General Discussion:

Before specific discussion of the Examiner's rejections, a brief summary of Le *vs.* the '320 Application may be helpful. Le is concerned with the well-known address ownership problem common to Internet Protocol version 6 ("Ipv6"), which uses 128-bit Internet addresses as a solution to the current shortage of 32-bit Ipv4 addresses. Le attempts to solve the address ownership problem by using a form of public-key encryption.

Public-key encryption, in general, is a system using one key known to all (the public key) and one private key known only to the recipient of a message. For example, if person A wants to send a secure message to person B, person A uses the public key to encrypt the message. Person B then uses his or her private key to decrypt the message.

Le uses public-key encryption to provide nodes of a network with keys (public and private) that are used to prove and verify ownership of an address. In particular, in Le, a first node ("N1"), e.g., a mobile node, has public and private keys. N1 generates an address (e.g., an Ipv6 address) using the public key. The public key is also known to a second node ("N2"). N2 sends an address verification request to N1, and N1 uses the private key to generate an address verification answer, proving to N2 that it owns the address. The address verification request may include a cookie or a challenge, such as a random number. N1's response is computed by applying the private key to the challenge, the cookie and/or the public key. See Le p. 2, ¶¶[0031]-[0033].

Le does not disclose authentication agents, prover agents or verifier agents, as discussed in the '320 Application. Le determines whether or not a node owns an internet address; however, Le does not determine whether or not a computer can be granted access to information on another computer (e.g., a host computer or other computer of a network). In addition, Le does not promote authenticated computers to perform authentication for a network. On the other hand, the '320 Application recites and claims each of the above features.

The '320 Application concerns authentication agents. An agent, as conventionally known, is a software program for collecting information and delivering the information over a network, or optionally, republishing the information in a standard format so that it can be collected over the network (e.g., by a central or host computer). See, e.g., Wikipedia Agentless Data Collection at http://en.wikipedia.org/wiki/Agentless_Data_Collection, under subheading entitled "What is an Agent?" In the '320 Application, verifier (or authentication) agents running within a secure network interact with prover agents within computers wishing to gain access to the network. Verifier and prover agents are created with initial values (i.e., for "s" and "n"). The agents read values published by a trusted source and decrypt the values, e.g., by a modulus inverse operation. The size of a resulting answer set is used to determine subsequent values. See Specification, pp. 4-6, ¶¶[0020]-[0025]. Through a series of challenge-response-verification iterations, a prover agent proves to the authentication agent that it is authorized to access, for example, a network or a secure area of a host computer. A connection is then established, and the computer running the prover agent is allowed access to the network of the secure area. Once

this connection is established, the computer running the prover agent may receive new values for "s" and "n", to maintain system integrity and security. Once a computer is authenticated and remains connected within the system, "it may operate to authenticate other computers (i.e., may operate as an authentication agent). Further, once authenticated and connected within system 500, the computer may operate to interact with other computers seeking authentication, enabling communication between the other computers and an authentication agent." Specification p. 8, ¶[0032]; see also pp. 6-8, ¶¶[0026]-[0031].

Claims 1-13:

Turning now to the claims, we note that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). However, Le does not expressly or inherently describe each and every element of claims 1-13. For example:

Independent claim 1 recites a method of non-centralized zero-knowledge authentication for a computer network, including the following steps:

(a) establishing a first computer having a first authentication agent and a first prover agent on the computer network;

(b) detecting a first authentication request over the computer network from a second computer having a second prover agent;

(c) authenticating the second prover agent through a zero-knowledge identification protocol; and

(d) promoting the second computer with a second authentication agent to perform authentication for the computer network.

As noted in the general discussion above, Le does not disclose (a) authentication agents or prover agents. Rather, Le discusses public-key encryption using public and private key pairs, which are used for address verification, and not for performing authentication for a computer network. Furthermore, Le fails to teach or even suggest (d) promoting a second computer to perform authentication for a computer network. For example, Le discusses address verification

performed between nodes (e.g., between a correspondent node and a mobile node), but nowhere discloses or even hints that once verified, a node can perform any type of authentication for other nodes. For example, Le does not discuss verification between mobile nodes. Rather, "the embodiments described aim at solving the need for a Mobile IPv6 MN to be able to send securely Binding Update messages to Correspondent Nodes with which no previous security associations exist, and in particular ***the CN needs to be able to verify that the MN owns the Home Address and the Care-of Address*** in the Binding Update message." Le p. 3, ¶[0044], emphasis added. The verification of an address used within a Binding Update message is not equivalent to the authentication of step (c).

Since Le does not teach or suggest all of the elements of claim 1, there can be no anticipation. We respectfully request withdrawal of the Examiner's rejection.

Claims 2-4: These claims depend from claim 1, and thus benefit from like argument. However, claims 2-4 contain additional unique features that are not disclosed in Le. For example, claim 2 recites periodically generating and distributing a new secret to the first and second authentication agents. As described in the '320 Application, "[t]he frequency of updates is less than the predicted length of time a malicious party could factor product or guess secret." Specification p. 4, ¶[0013]. Claim 4 recites periodically publishing encrypted numbers for the zero-knowledge identification protocol, including publishing encrypted values of the secret and product. Contrary to the Examiner's assertion, we do not find such *periodic* generation at Le paragraphs ¶¶[0112]-[0126], or elsewhere. Furthermore, Le teaches away from periodic security measures (e.g., RR tests), pointing to cost and bandwidth limitations caused by such measures in other internet protocol version 6:

> "...every time MN (Mobile Node) wants to send a BU, it needs to perform the RR test which requires seven messages to be sent over the air interface. In wireless links, this is unacceptable. In addition, the lifetime of the RR test is only 5 minutes; and the RR tests then needs to be re-executed. This large number of required messages is a major constraint for wireless networks where bandwidth is limited and expensive. In addition this RR test must be frequently (periodically) re-executed to prevent potential future attacks." Le p. 1, ¶[0012]; and
>
> "In the context of Mobile IPv6, in order to solve this problem, the MN and the CN must frequently perform the RR test but this protocol requires 7 messages to

> be exchanged; and this test must be performed not only when the MN changes its CoA but also periodically. The number of messages thus required, is a problem for wireless networks where bandwidth is limited and expensive." Le p. 2, ¶[0015]

Claim 3 recites authenticating a third prover agent and promoting a third computer with a third authentication agent, to perform authentication for the computer network. Again, Le does not disclose promoting computers to perform authentication for a network. See arguments in support of claim 1 step (d), above.

Le does not teach or suggest all of the elements of claims 2-4; hence, anticipation is not established. We respectfully request withdrawal of the Examiner's rejection.

Independent Claim 5: As amended, claim 5 recites a method of protecting a host from unauthorized client access over a network, including the following steps (among others):

(a) installing a prover agent application on the client;

(b) installing a verifier agent application on the host; and

(c) performing a plurality of verification dialog between the prover and verifier, wherein the prover demonstrates knowledge of the secret and product without exposing the values of the secret and product, and ***wherein the client is denied access to a secure area of a the host when the prover fails to demonstrate knowledge of the secret and product and granted access to the secure area when the client succeeds in demonstrating knowledge of the secret and product.***

Support for installation of prover and verifier agent applications may be found at claim 12 (reciting installation of prover and authentication agents through software). In addition, "[to] enable this non-centralized zero knowledge authentication, authentication software (including authentication and prover agents) may be preloaded into each computer (e.g., computers 514, 516, 518, 530, 534, 536)." Specification pp. 8-9, ¶[0033]. Note also that an authentication agent may be a verifier. See, e.g., Specification pp. 6-7, ¶¶[0026] and [0029].

Support for denying and granting access to a secure area of a host may be found at Specification pp. 6-7, ¶¶[0026]-[0027]; FIG. 4.

Le does not disclose installing prover or verifier agent applications on clients and hosts, as in elements (a) and (b). Nor does Le disclose denying or granting access to a secure area of a

host, based upon knowledge of a secret. Again, Le teaches address verification, and does not make any mention of allowing and/or denying access to any host. Since Le fails to teach at least the above elements of claim 5, the §102 rejection fails. Accordingly, we respectfully request withdrawal of the rejection of claim 5.

Claims 6 and 7: These claims depend from claim 5, and benefit from the above arguments. In addition, claim 6 recites utilizing previous values of a secret and product as operators in modulus inverse operations, in the steps of decrypting the secret and product. Since Le does not disclose periodic distribution of the secrets and product, Le cannot disclose the use of the previous values of the secret and product to decrypt the new values.

Claim 7 recites installing first and second agents. Respectfully, the paragraphs cited by the Examiner appear to discuss generation of public and private keys. This is different from installing agents, as in amended claim 7.

Given the above arguments and the arguments presented in support of base claim 5, Le does not anticipate claims 6 and 7. Withdrawal of the Examiner's §102 rejection is respectfully requested.

Independent Claim 8: Claim 8 recites a system of non-centralized zero-knowledge authentication for a computer network. Among other features, claim 8 recites two or more computers establishing the computer network, each of the computers containing an authentication agent, secret and prover agent. A requesting computer has a prover agent, for requesting access to the computer network.

As noted above, Le does not disclose Applicants' authentication and prover agents. Furthermore, Le verifies IP addresses, and does not disclose control of access to a computer network, or requesting such access. Le therefore fails to disclose, or even suggest, all of the features of claim 8; hence, there can be no anticipation. Withdrawal of the Examiner's rejection is respectfully requested.

Claims 9-12: Claims 9-12 depend from claim 8 and benefit from like argument. Furthermore, claim 9 recites a trusted source for periodically generating a new secret for authentication agents. As noted above, Le does not disclose Applicants' authentication agents.

In addition, Le teaches away from periodically-performed security measures. See arguments in support of claims 2-4, above.

Claim 12 recites authentication agents and prover agents being installed on each of the computers through common software. Again, Le does not teach or suggest installing agents on software. Le paragraphs [0142]-[0147], which the Examiner cites in support of his contrary position, discuss computation of secrets by each entity. There is no mention of software installation. Notably, the words "software," "install," and "load" are all absent from Le.

Claims 9-12 are not anticipated by Le. We respectfully request withdrawal of the Examiner's rejection.

Independent Claim 13: This claim recites a software product comprising instructions, stored on computer-readable media, wherein the instructions, when executed by a computer, perform steps for non-centralized zero-knowledge authentication for a computer network, including:

(a) instructions for establishing a first computer having a first authentication agent and a first prover agent on the computer network;

(b) instructions for detecting a first authentication request over the computer network from a second computer having a second prover agent;

(c) instructions for authenticating the second prover agent through a zero-knowledge identification protocol; and

(d) instructions for promoting the second computer with a second authentication agent to perform authentication for the computer network.

Le does not disclose each of elements (a)-(d). For example, Le does not disclose Applicants' authentication and prover agents. Furthermore, Le does not mention software, even once. Finally, Le does not promote a computer to perform authentication for a network. See arguments in support of claim 1, above.

CONCLUSION

We believe that the above amendments and the remarks laid out below address and overcome the objection and each of the rejections presented in the Office Action mailed 26 March 2007. We respectfully request the Examiner's consideration of the amendments presented herein. We likewise request withdrawal of the rejections presented in the 26 March Office Action, and allowance of claims 1-13.

This application is filed with a Petition for 3 months' extension and authorization to charge the required fees to Deposit Account No. 12-0600. This extends the period for reply up to and including September 26, 2007. Hence, this Amendment and Response is timely filed. No other fees are believed due; however, if any additional fee is deemed necessary in connection with this Amendment and Response, please charge Deposit Account No. 12-0600. Should any issues remain outstanding, the Examiner is encouraged to telephone Applicants' attorney, Curtis A. Vock, at (720) 931-3011.

Respectfully submitted,
LATHROP & GAGE L.C.

Date: 26 Sept. 2007

By: Heather Perrin

Heather F. Perrin, Reg. No. 52,884
4845 Pearl East Circle, Suite 300
Boulder, Colorado 80301
Telephone: (720) 931-3033
Facsimile: (720) 931-3001